УДК 004.415.2.043

АНАЛИЗ МОДЕЛЕЙ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ

Кононенко В.И.
Научный руководитель – к.т.н., профессор Варлатая С.К.

Дальневосточный государственный технический университет

Одной из кардинальных проблем теории защиты информации является развитие методов оценки защищенности информации. Сложность ее решения обусловлена целым рядом факторов:

отсутствие формальных моделей угроз безопасности;

наличие ряда факторов неопределенности;

различие в оценках негативных последствий от реализации одних и тех же угроз на разных объектах информатизации;

отсутствие шкал для количественной оценки некоторых видов ущерба;

неполнота данных об исследуемых процессах;

не линейности исследуемых процессов.

Каждая угроза безопасности информации в компьютерной системе рассматривается за период с некоторой вероятностью относительно одного или нескольких блоков защищаемой информации. В ходе это процесса может быть выполнено одно из множества деструктивных действий: уничтожение, копирование, модификация информации и т. д. Разные виды ущерба оцениваются как в количественных, так и в качественных шкалах. В данной статье рассмотрены следующие основные модели оценки защищенности информации: модель анализа рисков, аддитивная модель, порядковая шкала и модель решетки ценностей.

При использовании аддитивной модели, определение ценности базируется на экспертных оценках компонент данной информации, и при объективности денежных оценок её компонент, подсчитывается искомая величина. Основная проблема заключается в том, что количественная оценка компонент информации часто оценивается необъективно даже при её оценке высококвалифицированными специалистами. Причина заключается в неоднородности компонент информации в целом. Для решения этой проблемы принято использовать иерархическую относительную шкалу, которая представляет из себя линейный порядок, с где сравниваются отдельные компоненты защищаемой информации по ценности одна относительно другой. Случай единой шкалы равносилен тому, что все компоненты, имеющие равную порядковую оценку, равноценны одна относительно другой.

В том случае, когда установить соответствие ценности информации к денежному эквиваленту не представляется возможным, тогда имеет смысл сравнительная оценка отдельных информационных компонент. В качестве примера рассмотрим ситуацию, которая имеет местов государственных структурах, где информация разбивается по грифам секретности, грифы секретности представляют собой порядковые шкалы ценностей, такие как: несекретно, для служебного пользования, секретно, совершенно секретно, особой важности. Чем выше класс грифа, тем большую ценность имеет защищаемая информация, в связи с чем по отношению к ней применяются более высокие требования по её защите от несанкционированного доступа.

Модель анализа риска основывается на уже известных данных о стоимостях компонент информации, исходя из прогнозирования возможных угроз для информации. Вероятность каждой угрозы оценивается с помощью статистических

оценок соответствующих событий. Подсчитывается сумма математических ожиданий потерь для каждой из компонент по закону распределения возможных угроз.

Модель решётки ценностей - это обобщение порядковой шкалы. Предположим, что дано M — конечное частично упорядоченное множество относительно бинарного отношения < , то есть для каждых A, B и C выполняется:

Рефлективность: A > A

Транзитивность: A < B, B < C то A < C

Антисимметричность: A < B, B < B то A = B

Для любого A и B принадлежащих множеству M элемент C = A □ B □ C называется наименьшей общей гранью, если:

A < C, B < C

A < D, B < D то C < D для всех D принадлежащих множеству M

При этом необязательно существование самого элемента A □ B Если выполнено условие существования наименьшей верхней границы, то из антисимметричности следует единственность. По определению, элемент E = A □ B □ C называется наибольшей нижней границей для A, B □ C (нижней гранью), если

E < A, E < B

D < A, D < B то D < E

Существование нижней границы не является обязательным, но если она существует, то из антисимметричности следует единственность.

Существующие модели оценки защищенности информации являются узкоспециализированными, поэтому выбор необходимой модели базируется исключительно на специфики области его применения.